The Cost of Security: Firewall Focus

2011 Computer System, Cluster, and Networking Summer Institute

Team Members: Charles "David" Warner, Kyle Sandoval, Estevan Trujillo

Mentors: Alex Malin, Susan Coulter, Ed Brown

Los Alamos NATIONAL LABORATORY EST. 1943

Objective

The IPTables firewall is a tremendously powerful tool that is utilized by some of LANL's various computer networks for security. This tool allows administrators to define exactly what types of traffic are allowed to enter or exit any host on the network. It also allows administrators to log specific types of traffic. Currently the cost of using IPTables on every compute node in the cluster lacks thorough research. In this project, we create multiple IPTables rule sets and run a series of benchmarking tools that measure bandwidth, latency, and CPU performance. The purpose of these tests test is to try to determine what performance implications IPTables has on a cluster. This effect ended up being negligible for moderately sized rule sets on slower interconnects and less than expected on faster interconnects.

Tools Used

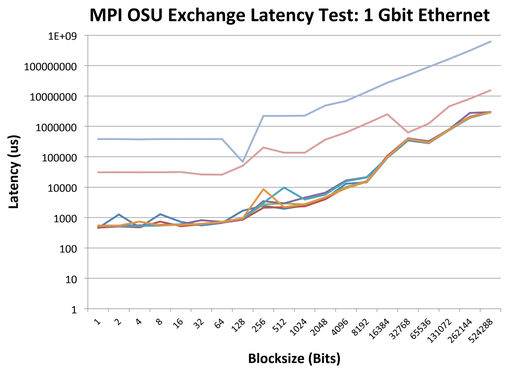
Our primary benchmarking tools include:

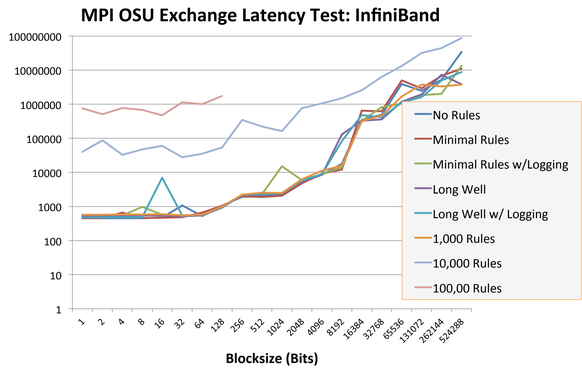
Iperf, which measures the throughput of a network by creating TCP and UDP data streams that flow through the network, thus measuring the cluster's bandwidth.

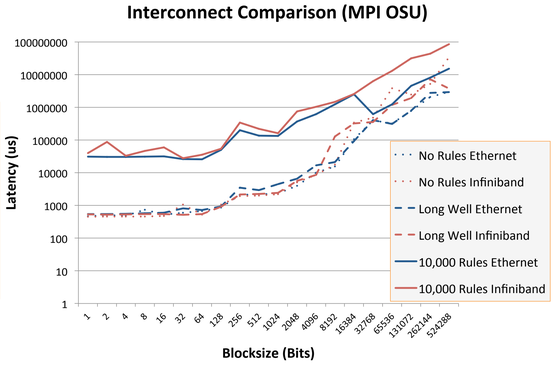
OSU Micro-Benchmarks, which monitor latency and bandwidth, including bidirectional, multiple, and multi-pair.

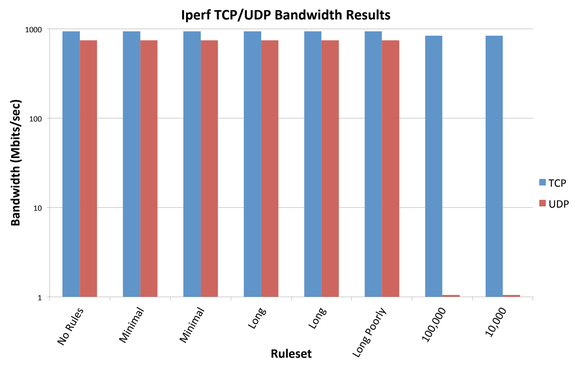
Methods

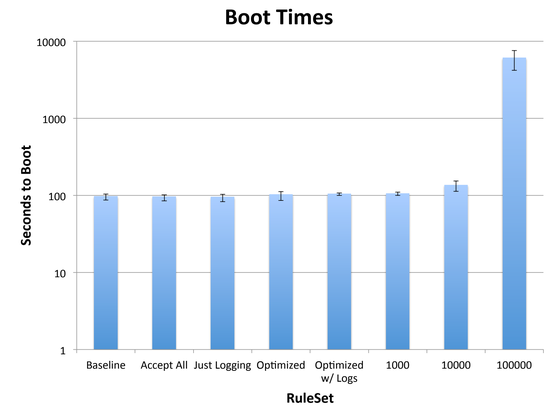
The first task that we completed during the course of this project was to get our CentOS cluster up and running. Once this was done, we created our various IPTables rule sets, resulting in eight different rule sets to be tested. The first test was set with IPTables turned off to establish a baseline, followed by a minimal rule set, a minimal rule set with logging, a long well-written rule set, a long well-written rule set with logging, a long rule set which was poorly written, and two long rule sets (one with 100,000 rules and another with 10,000 rules). Each test was conducted using every rule set, across all our nodes, multiple times to make sure that the data accrued from the results was consistent.

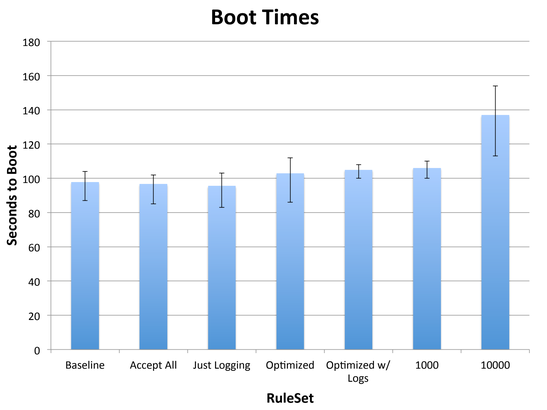












Results

Our tests on 1 Gigabit interconnects have concluded that running IPTables on each of the computer nodes in a cluster has very little effect on performance. Results showed that it had no noticeable effect on bandwidth utilization through the cluster and showed that the data rate was the same no matter which rule set we were using. The OSU Benchmark results showed that there were statistically irrelevant differences that occurred between the various rule sets we tested.

Further Research

Interesting potential future experiments include finding the impact that various high speed interconnects would have on the results, such as Infiniband, 10 Gig Ethernet and 40 Gig Ethernet. Seeing what kind of performance implications ACLs set up on the switch would also be very interesting. Additionally, it would be nice to explore the financial cost that these performance implications would cost both in terms of additional hardware and labor.

Recommendations

As a result of these tests our team has concluded that running IPTables on compute nodes in a cluster that is using a 1 Gigabit interconnect has a negligible effect of the performance of a cluster using a moderately sized rule set.

Contact Info

Charles "David" Warner, cdwarner@mtu.edu

Kyle Sandoval, sandoval.kyle@gmail.com

Estevan Trujillo, etrujill@nmt.edu

ISTI INFORMATION SCIENCE & TECHNOLOGY INSTITUTE

National Security Education Center — A CONSORTIUM OF LANL INSTITUTES

LA-UR-11-11196

New Mexico CONSORTIUM — NM State, New Mexico Tech, The University of New Mexico

PRObE Parallel Reconfigurable Observational Environment

NSF